UNITED
NATIONS

A

General Assembly

Distr.
LIMITED

A/CN.9/WG.IV/WP.79
23 November 1998

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-fourth session
Vienna, 8-19 February 1999

DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Note by the Secretariat

CONTENTS

	Paragraphs	Page
INTRODUCTION	1-11	3
I. GENERAL REMARKS	12-14	4
II. DRAFT PROVISIONS ON DIGITAL SIGNATURES, OTHER ELECTRONIC SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES	15-53	5
CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS	15-20	5
CHAPTER II. ELECTRONIC SIGNATURES	21-48	7
Section I. Electronic signatures in general	21-23	7
Article 1. Definitions	21	7
Article 2. Compliance with requirements of law	22-23	9

V.98-57598

	Paragraphs	Page
Section II. [Enhanced][Secure] electronic signatures . .	24-44	10
Article 3. [ ]	24-30	10
Article 4. Presumption of attribution of [enhanced] electronic signature	31-33	12
Article 5. Presumption of integrity	34-37	13
Article 6. Pre-determination of [enhanced] electronic signature	38-41	14
Article 7. Liability for unauthorized use of [enhanced] electronic signature	42-44	15
Section III. Digital signatures supported by certificates		
Article 8. Contents of [enhanced] certificate	45-48	18
Article 9. Effect of digital signatures supported by certificates	47-48	20
CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES	49-53	22
Article 10. Undertaking upon issuance of [enhanced] certificate	49-50	22
Article 11. Contractual liability	51	24
Article 12. Liability of the certification authority to parties relying on certificates	52	25
General remark regarding draft articles 13 to 15	53	26
Article 13. Revocation of certificate	--	26
Article 14. Suspension of certificate	--	27
Article 15. Register of certificates	--	27

INTRODUCTION

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [1]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). The Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While no firm decision as to the form and content of such work had been reached, the Working Group had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157).

3. The Commission endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities (hereinafter referred to as "the Uniform Rules").

4. With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce (the Model Law). Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [2]

5. The Working Group began the preparation of the Uniform Rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73).

6. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). The Commission expressed its appreciation of the efforts accomplished by the Working Group in its preparation of draft Uniform Rules on Electronic Signatures. It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the draft Uniform Rules on Electronic Signatures were progressively being shaped into a workable structure.

7. The Commission reaffirmed the decision made at its thirty-first session as to the feasibility of preparing such Uniform Rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session (New York, 29 June-10 July 1998) on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues.

8. The Working Group continued revision of the Uniform Rules at its thirty-third session (1998) on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.76). The report of the session is contained in document A/CN.9/454.

9. This note contains the revised draft provisions prepared pursuant to the deliberations and decisions of the Working Group and also pursuant to the deliberations and decisions of the Commission at its thirty-first session, as reproduced above. They are intended to reflect the decisions made by the Working Group at its thirty-third session.

10. In the preparation of this note, the Secretariat was assisted by a group of experts, comprising both experts invited by the Secretariat and experts designated by interested governments and international organizations.

11. In line with the applicable instructions relating to the stricter control and limitation of United Nations documents, the explanatory remarks to the draft provisions have been kept as brief as possible. Additional explanations will be provided orally at the session.

I. GENERAL REMARKS

12. The purpose of the Uniform Rules, as reflected in the draft provisions set forth in part II of this note, is to facilitate the increased use of electronic signatures in international business transactions. Drawing on the many legislative instruments already in force or currently being prepared in a number of countries, these draft provisions aim at preventing disharmony in the

legal rules applicable to electronic commerce by providing a set of standards on the basis of which the legal effect of digital signatures and other electronic signatures may become recognized, with the possible assistance of certification authorities, for which a number of basic rules are also provided.

13. Focused on the private-law aspects of commercial transactions, the Uniform Rules do not attempt to solve all the questions that may arise in the context of the increased use of electronic signatures. In particular, the Uniform Rules do not deal with aspects of public policy, administrative law, consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures.

14. Based on the Model Law, the Uniform Rules are intended to reflect in particular: the principle of media-neutrality; an approach under which functional equivalents of traditional paper-based concepts and practices should not be discriminated against; and extensive reliance on party autonomy. They are intended for use both as minimum standards in an "open" environment (i.e., where parties communicate electronically without prior agreement) and as default rules in a "closed" environment (i.e., where parties are bound by pre-existing contractual rules and procedures to be followed in communicating by electronic means).

II. DRAFT PROVISIONS ON DIGITAL SIGNATURES, OTHER ELECTRONIC SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES

CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS

15. In considering the draft provisions proposed for inclusion in the Uniform Rules, the Working Group may wish to consider more generally the relationship between the Uniform Rules and the Model Law. In particular, the Working Group might wish to make proposals to the Commission as to whether uniform rules on digital signatures should constitute a separate legal instrument or whether they should be incorporated in an extended version of the Model Law, for example as a new part III of the Model Law.

16. If the Uniform Rules are prepared as a separate instrument, it is submitted that they will need to incorporate provisions along the lines of article 1 (Sphere of application), article 2 (definitions as required), article 3 (Interpretation) and article 4 (Variation by agreement) of the Model Law. While those articles are not reproduced in this note, it should be noted that the draft provisions of the Uniform Rules have been prepared by the Secretariat on the assumption that such provisions would be included in the Uniform Rules. With respect to the sphere of application of the Uniform Rules, it should be borne in mind that, if an article along the lines of article 1 of the Model Law is included, transactions involving consumers would not be excluded from their sphere of application unless the law applicable to consumer transactions in the enacting State conflicted with the Uniform Rules.

17. As to the question of party autonomy, a mere reference to article 4 (Variation by agreement) of the Model Law may not suffice to provide a satisfactory solution. Article 4 establishes a distinction between those provisions of the Model Law that may be freely varied

by contract and those provisions that should be regarded as mandatory unless variation by agreement is authorized by the law applicable outside the Model Law. With respect to electronic signatures, the practical importance of "closed" networks makes it necessary to provide wide recognition of party autonomy. However, public policy restrictions on freedom of contract, including laws protecting consumers from overreaching contracts of adhesion, may also need to be taken into consideration. The Working Group may thus wish to include in the Uniform Rules a provision along the lines of article 4(1) of the Model Law to the effect that, except as otherwise provided by the Uniform Rules or other applicable law, electronic signatures and certificates issued, received or relied upon in accordance with procedures agreed among the parties to a transaction are given the effect specified in the agreement. In addition, the Working Group might consider establishing a rule of interpretation to the effect that, in determining whether a certificate, an electronic signature or a data message verified with reference to a certificate, is sufficiently reliable for a particular purpose, all relevant agreements involving the parties, any course of conduct among them, and any relevant trade usage should be taken into account.

18. In addition to the above-mentioned provisions, the Working Group may wish to consider whether a preamble should clarify the purpose of the Uniform Rules, namely to promote the efficient utilization of electronic communication by establishing a security framework and by giving written and electronic messages equal status as regards their legal effect.

19. At its thirty-third session, the Working Group expressed doubts as to the appropriateness of using the terms "enhanced" or "secure" to describe signature techniques that were capable of providing a higher degree of reliability than "electronic signatures" in general (A/CN.9/454, paras. 29). The Working Group concluded that, in the absence of a more appropriate term, "enhanced" should be retained. For those reasons, "enhanced" is included in this revision of the Uniform Rules in square brackets.

20. In discussing the relationship between these Uniform Rules and article 7 of the Model Law, the Working Group may wish to consider whether these Rules should be limited in their application to situations where there are legal form requirements or where the law provides for consequences in the absence of certain conditions, such as writing or a signature. It should be recalled that what is meant by form requirements was discussed in the preparation of the Model Law. Paragraph 68 of the Guide to Enactment of the Model Law notes that the use of the phrase "the law" in the Model Law is to be understood as encompassing not only statutory or regulatory law, but also judicially-created law and other procedural law. Thus the phrase "the law" also covers rules of evidence. Where the law does not stipulate a requirement for a particular condition, but provides for consequences in the absence of the condition, for example writing or signature, this is also to be included within the concept of "the law" as used in the Model Law.

CHAPTER II. ELECTRONIC SIGNATURES

Section 1. Electronic signatures in general

Article 1. Definitions

For the purposes of these Rules:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signer of the data message and indicate the signer's approval of the information contained in the data message][satisfy the conditions set forth in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce];

(b) "[Enhanced] electronic signature" means an electronic signature which [is created and][as of the time it was made] can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:

(i) is unique to the signer [for the purpose for][within the context in] which it is used;

(ii) can be used to identify objectively the signer of the data message;

(iii) was created and affixed to the data message by the signer or using a means under the sole control of the signer; [and]

[(iv) was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed].

(c) *Variant A*

"Digital signature" means an electronic signature created by transforming a data message using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key, such that any person having the initial untransformed data message, the encrypted transformation, and the signer's corresponding public key can [accurately] determine:

(i) whether the transformation was created using the private key that corresponds to the signer's public key; and

(ii) whether the initial data message has been altered since the transformation was made.

Variant B

"Digital signature" is a cryptographic transformation (using an asymmetric cryptographic technique) of the numerical representation of a data message, such that any person having the data message and the relevant public key can determine:

(i) that the transformation was created using the private key corresponding to the relevant public key; and

(ii) that the data message has not been altered since the cryptographic transformation.

(d) "Certification authority" means any person who, or entity which, in the course of its business, engages in issuing [identity] certificates in relation to cryptographic keys used for the purposes of digital signatures. [This definition is subject to any applicable law which requires a certification authority to be licensed, to be accredited, or to operate in a manner specified in such law.]

(e) "[Identity] certificate" means a data message or other record which is issued by a certification authority and which purports to confirm the identity [or other significant characteristic] of a person or entity who holds a particular key pair.

(f) "[Enhanced] certificate" means a[n identity] certificate issued for the purpose of supporting [enhanced][secure] electronic signatures.

(g) "Certification practice statement" means a statement published by a certification authority that specifies the practices that the certification authority employs in issuing and otherwise handling certificates.

(h) "Signer" means the person by whom, or on whose behalf, [an electronic signature is used][data is used as an electronic signature].

References

A/CN.9/454, para. 20;
A/CN.9/WG.IV/76, paras. 16-20;
A/CN.9/446, paras. 27-46 (draft article 1), 62-70 (draft article 4), 113-131 (draft article 8), 132-133 (draft article 9);
A/CN.9/WG.IV/WP.73, paras. 16-27, 37-38, 50-57, and 58-60;
A/CN.9/437, paras. 29-50 and 90-113 (draft articles A, B and C); and
A/CN.9/WG.IV/WP.71, paras. 52-60.

Remarks

21. At its previous session, for lack of sufficient time, the Working Group postponed its consideration of draft article 1 to a future session (see A/CN.9/454, para. 19). With the

exception of the deletion of the word "secure" in relation to electronic signatures, the text of draft article 1 in this note is identical to the text of that draft article as set forth in A/CN.9/WG.IV/76.

Article 2. Compliance with requirements of law

(1) With respect to a data message authenticated by means of an electronic signature [other than an [enhanced] electronic signature], the electronic signature meets any requirement of law for a signature if the method used to affix the electronic signature is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) Unless expressly provided elsewhere in [this Law], electronic signatures that are not [enhanced] electronic signatures are not subject to the regulations, standards, or licensing procedures established by ... *[the State-specified organs or authorities referenced in draft article 6]* or to the presumptions created by articles 3, 4 and 5.

(4) The provisions of this article do not apply to the following: [...].

References

A/CN.9/454, paras. 21-27;
A/CN.9/WG.IV/WP.76, para. 21; and
A/CN.9/446, paras. 27-46 (draft article 1).

Remarks

22. The purpose of draft article 2 is to confirm the connection between article 7 of the Model Law and the Uniform Rules. Draft article 2(1) includes the appropriate recognition of party autonomy. The Working Group may wish to consider whether the words included in square brackets in draft article 2(1) ["other than an enhanced electronic signature"] should be retained as they suggest that an enhanced electronic signature does not meet the requirement of article 7 of the Model Law. This appears to contradict the effect of Variant B of draft article 3.

23. Draft article 2(2) is included for consistency with article 7 of the Model Law and for the reasons noted above in relation to the meaning of the phrase "the law". Draft article 2(3) makes it clear that rules applying to higher levels of "enhanced" or "secure" electronic signatures, such as those relating to possible licensing schemes for certification authorities or other possible regulation for digital signatures for example, do not apply in general to all types of "electronic signatures".

Section II. [Enhanced] electronic signatures

Article 3.

Variant A

Article 3. Compliance of [enhanced] electronic signature with requirements of law

(1) Where the law requires a signature, that requirement is met by an [enhanced] electronic signature, [unless it is proved that the [enhanced] electronic signature does not fulfil the requirements of article 7 of the Model Law].

(2) Paragraph (1) applies whether the requirement referred to is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

Variant B

Article 3. Presumption of signing

(1) A data message is presumed to have been signed if an [enhanced] electronic signature is affixed to or logically associated with the data message.

(2) The provisions of this article do not apply to the following: [...].

Variant C

Article 3. Consequences arising from the use of an [enhanced] electronic signature

(1) Where consequences in law would arise from [the use of] a signature, those consequences arise from an [enhanced] electronic signature.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/454, paras. 28-39;
A/CN.9/WG.IV/WP.76, paras. 22-23;
A/CN.9/446, paras. 47-48 (draft article 2) and 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 28-36; and
A/CN.9/437, paras. 43, 48 and 92.

Remarks

Variant A

24. Variant A provides a rule for enhanced electronic signatures that is a shortcut to satisfying the requirements of article 7 of the Model Law. This Variant of draft article 3 and draft article 2 establish the basis of the Uniform Rules. Firstly, draft article 2 restates the principle of article 7 of the Model Law that an electronic signature can satisfy a requirement of law for a signature provided that it meets certain conditions. Second, Variant A of draft article 3 provides that an [enhanced] electronic signature does meet those conditions and a shortcut to satisfying the requirement of article 7 is established.

25. The provision which confirms that the phrase "the law" applies whether the requirement is in the form of an obligation or whether the law simply provides consequences for the absence of a particular condition has been repeated in paragraph (2) of Variant A, to ensure that the meaning of the phrase "the law" is consistent between with the draft Uniform rules and the Model Law.

26. If the words in square brackets in draft Variant A are retained, draft Variant A provides a shortcut to satisfying the requirements of article 7 of the Model Law, which may be qualified where proof is introduced to show that the requirements of article 7 are not satisfied. The Working Group may wish to consider whether those words should be retained in draft article 3.

Variant B

27. The purpose of Variant B is to create a presumption that a data message can be regarded as "signed" if it is authenticated by an enhanced electronic signature. As such, this presumption treats the "signing" of a message as being distinct from the question of the identification of the signer. Such a presumption may be important where there is no formal requirement for a signature, as set out in article 7 of the Model Law, but where the existence of a signature on a data message may be important for some other purpose, or in cases where the law requires that a message be signed without specifying the identity of the signer or where the signer's identity is not at issue.

28. As currently drafted, Variant B may apply to situations additional to those contemplated by article 7. The Working Group may wish to consider whether these two arms of article 7 (i.e., where there is a requirement of law for a signature or where consequences are specified in the absence of a signature) catch all situations where a signature could be used and have legal effect. If they do not, a provision along the lines of Variant B may be useful. In such circumstances, Variant B may be retained together with Variant A, as Variant B will deal with additional circumstances.

29. The reference in the previous draft of article 3 to the time at which the signature was affixed has been deleted, but the Working Group may wish to consider whether this concept may need to be included elsewhere in the draft Uniform Rules.

Variant C

30. The purpose of this variant is to establish in the Uniform Rules a clear principle of non-discrimination, as reflected in article 5 of the Model Law. The provision is intended to ensure that where the use of signature gives rise to legal consequences, irrespective of a formal requirement for a signature, those consequences will be the same for both handwritten and electronic signatures. The effect of this Variant is very close to that of Variant B, as both rely on domestic law to provide the consequences where a message is signed (Variant B) or a signature has been used (Variant C).

Article 4. Presumption of attribution of [enhanced] electronic signature

(1) An [enhanced] electronic signature is presumed to be that of the person by whom, or on whose behalf, it purports to have been generated, unless it is established that the [enhanced] electronic signature was applied neither by the purported signer nor by a person who had the authority to act on its behalf.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/454, paras. 40-53;
A/CN.9/WG.IV/WP.76, paras. 24;
A/CN.9/446, paras. 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 33-36;
A/CN.9/437, paras. 118-124 (draft article E); and
A/CN.9/WG.IV/WP.71, paras. 64-65.

Remarks

31. Draft article 4 provides a presumption of attribution for [enhanced] electronic signatures, and provides two cases where the presumption does not apply. As such, it deals with issues addressed in article 13 of the Model Law, although there are some differences in its drafting. Draft article 4, for example, is in the form of a rebuttable presumption of attribution. Article 13(2) of the Model Law, on the other hand, is in the form of a deeming provision, and article 13(3) establishes a rule entitling the addressee to act on the attribution of the data message. Draft article 4 deals with attribution of a signature, while article 13 of the Model Law is concerned with attribution of the data message. The tests for attributing the signature in draft article 4 are slightly different to the criteria used in article 13 of the Model Law for attributing the data message.

32. The Working Group may wish to consider the relationship between draft article 4 and article 13 of the Model Law and in particular, whether there is any legal need for a distinction to be drawn between attribution of the message and attribution of the signature on that message. It should be borne in mind that for technical reasons, it may not be possible for such a

distinction to be made. It may be that attribution of a signature should follow attribution of a data message, or vice versa and only one rule on attribution is needed.

33. Another aspect of draft article 4 is that it deals with unauthorised use of the electronic signature. In that respect it overlaps with issues covered by article 13 of the Model Law. Draft article 4, for example, provides that the presumption of attribution does not apply in two instances - where the signature was applied neither by the purported signer nor by a person authorised by the purported signer. Article 13, on the other hand, provides that notwithstanding that the message was unauthorised, the addressee may regard the data message as being that of the purported originator. The Working Group may wish to consider the need for including a new rule on the unauthorized use of signatures in these Uniform Rules and the relationship of such a rule to draft article 7 on liability.

Article 5. Presumption of integrity

(1) *Variant A*

Where [a trustworthy security procedure] [an enhanced electronic signature] is properly applied to a designated portion of a data message and indicates that the designated portion of the data message has not been changed since a specific point in time, it is presumed that the designated portion of the data message has not been changed since that time.

Variant B

Where a security procedure is capable of showing [reliably] [with substantial certainty] that the designated portion of a data message has not been changed since a specific point in time, and a proper application of that procedure indicates that the data message has not been changed, it is presumed that [the integrity of the data message has been preserved] [the data message has not been changed] since that time.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/454, paras. 54-63;
A/CN.9/WG.IV/WP.76, paras. 25-26;
A/CN.9/446, paras. 47-48 (draft article 2);
A/CN.9/WG.IV/WP.73, paras. 28-32; and
A/CN.9/437, paras. 43, 48 and 92.

Remarks

34. Draft article 5 has been revised in accordance with the decision of the Working Group at its thirty-third session (A/CN.9/454, paras. 54-63). The revised draft purports to establish a presumption as to integrity of the data message. In order to establish the presumption both

variants of the draft article appear to require that the security procedure or signature must actually have been applied with a result which shows that there has been no change to the message. Once this evidence is available, little value could be attached to a presumption to that effect. The Working Group may wish to consider whether the draft article should be drafted as a presumption or as a substantive rule of law.

35. One of the alternatives provided in Variant A is based upon the application of the signature as indicating integrity. The Working Group may wish to consider whether both the application and the verification of that signature (and the use of the hash function or message digest) should be included or whether the application of a security procedure is a preferable formulation.

36. Draft article 5(1) of both Variants A and B makes a direct connection between the signing of a message and the integrity of that message, a connection which may not always be useful or necessary. In some cases, the integrity function is an integral part of the type of electronic signature technology used (as may be the case with particular types of [enhanced] electronic signatures), and a presumption as to integrity simply states what is a direct result of the use of that technology. In other cases, the signature technology used may not be capable of satisfying a requirement for integrity, even though in all other respects such a signature may be considered to be an [enhanced] electronic signature. In addition, there will be cases where it may be necessary to prove the integrity of a message which is not signed. For such cases, a rule establishing a direct connection between integrity and signature may not be useful.

37. Where integrity is required in order to show that a message is an original, article 8 of the Model Law is relevant. The Working Group may wish to consider whether a presumption as to integrity should be included in these Rules as a substantive rule, whether the integrity function should be included in the definition of [enhanced] electronic signature and the relationship between this draft article and article 8 of the Model Law.

Article 6. Predetermination of [enhanced] electronic signature

(1) *[The organ or authority specified by the enacting State as competent]* may determine:

(a) that an electronic signature is [an [enhanced] electronic signature] [satisfies the requirements of article 7 of the Model Law];

[(b) that a security procedure satisfies the requirements of article 5].

(2) Any determination made under paragraph (1) should be consistent with recognized international technical standards.

(3) [Subject to [these Rules and] applicable law] parties may agree that an electronic signature is to be treated among themselves:

[(a) as an [enhanced] electronic signature];

[(b) as satisfying the requirements of article 7 of the Model Law].

References

A/CN.9/454, paras. 64-75
A/CN.9/WG.IV/WP.76, para. 27.
A/CN.9/446, paras. 37-45 (draft article 1); and
A/CN.9/WG.IV/WP.73, para. 27.

Remarks

38. The previous version of draft article 6(1) referred to the signature as satisfying the requirements of draft article 1(b) (the definition of [enhanced] electronic signature). This revision of draft article 6 allows for a determination that an electronic signature is an [enhanced] electronic signature or, as an alternative possibility, that the electronic signature satisfies the requirements of article 7, thereby establishing a clear shortcut. If an electronic signature is an [enhanced] electronic signature under Variant A of draft article 3, there is no need to state that it satisfies the requirements of article 7, since this is clear from its [enhanced] status.

39. The revised version of draft article 6(1)(b) agreed to at the thirty-third session of the Working Group (A/CN.9/454, para. 73) refers to the "requirements of article 5". As revised at the same session (A/CN.9/454, para. 61) draft article 5 no longer establishes requirements for integrity. The Working Group may wish to reconsider the inclusion of a reference to draft article 5 in draft article 6(1)(b).

40. In draft article 6(2) the words "to the extent that they exist" have been deleted on the basis that they are not necessary in the context of a Model Law. To the extent that such standards exist, States enacting the Uniform Rules should be encouraged to observe them and a note to this effect could be included, for example, in a guide to enactment.

41. The language of draft article 6(3) has been revised to reflect the concern expressed at the thirty-third session of the Working Group (A/CN.9/454, para. 71) that, while party autonomy should be respected, any agreement between parties as to the use of an electronic signature should not operate to affect third parties. The revision also addresses concerns (A/CN.9/454, para. 75) as to the use of the phrase "determine the effect of a signature" (emphasis added) and what that might mean in different legal systems. Draft paragraph (3) adopts the drafting of paragraph (1), providing the determination of [enhanced] status as an alternative to a determination that the signature meets the requirements of article 7 of the Model Law.

Article 7. Liability for unauthorized use of [enhanced] electronic signature

Variant A

Where the use of an [enhanced] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature,

Variant X the signature is nevertheless regarded as authorized, unless the relying party knew or should have known that the signature was not authorized.

Variant Y the purported signer may be held liable only for the cost of restoring the parties to their position before the unauthorized use of the signature, unless the relying party knew or should have known that the signature was not that of the purported signer.

Variant Z the purported signer is liable [to pay damages to compensate the relying party] for harm caused, unless the relying party knew or should have known that the signature was not that of the purported signer.

Variant B

(1) Where:

(a) the use of an [enhanced] electronic signature was unauthorized;

(b) the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such signature; and

(c) the addressee reasonably relied on the signature in good faith to its detriment

the signature is [attributed] [attributable] to the purported signer for the purpose of allocating responsibility for the cost of restoring the parties to their position prior to the unauthorized use of the signature.

(2) Paragraph (1) shall not apply to the extent that the addressee knew or should have known that use of the signature was unauthorized.

Variant C

(1) Where an [enhanced] electronic signature is affixed to a data message and:

(a) the use of the [enhanced] electronic signature was unauthorized;

(b) the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature; and

(c) the addressee reasonably relied on the signature in good faith to its detriment,

the data message shall be attributed to the purported signer unless it [is not just and equitable][would be manifestly unfair] to do so, having regard to the purposes for which the data message was used and other relevant circumstances.

(2) [Where subparagraphs (a), (b) and (c) of paragraph (1) apply, and the data message is not attributed to the purported signer under paragraph (1)][Where the data message is not attributed to the purported signer under paragraph (1) on the grounds of manifest unfairness], the purported signer is nevertheless liable for the cost of restoring the addressee to the position it occupied prior to the use of the unauthorised signature.

(3) Paragraph (1) shall not apply:

(a) to the extent that the addressee knew or should have known, had it exercised reasonable care, that the signature was not that of the purported signer;

(b) where the addressee received notice from the purported signer that the signature was not that of the purported signer and the addressee had a reasonable time to act accordingly.

(4) It would be manifestly unfair to attribute an unauthorised signature to a purported signer under paragraph (1) if:

(a) to do so would cause hardship to the purported signer out of proportion to the loss suffered by the addressee;

(b) [.....]

References

A/CN.9/454, paras. 76-88;
A/CN.9/WG.IV/WP.76, paras. 28-30;
A/CN.9/446, paras. 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 33-36;
A/CN.9/437, paras. 118-124 (draft article E); and
A/CN.9/WG.IV/WP.71, paras. 64-65.

Remarks

42. Draft article 7 has been revised to include a number of different Variants as discussed by the Working Group at its thirty-third session (A/CN.9/454, paras. 76-88). As currently drafted, Variants A and B both raise issues which are covered by article 13 of the Model Law, in particular under article 13(3). It should be noted, however, that article 13 of the Model Law deals with attribution of a data message, while draft article 7 deals with unauthorized use of a signature.

43. The way in which the issue of attribution is treated in draft article 7 is slightly different from the treatment under article 13. For example, under article 13(4)(a) and (b), where there is an unauthorized message within the meaning of article13(3)(b), the receiving party can rely upon the message, provided it has not received notice of the lack of authorization, or it should have known that the message was unauthorized. Article 13 does not specify that the purported signer can raise the defence that it acted reasonably to protect the signature (i.e., by preventing access to a method used by the signer to identify the data message as its own), which it can do under Variant B(1)(b) of draft article 7. In addition, article 13 does not address the issue of the relying party acting in good faith to its detriment; in contrast, it is clear that Variant B(1)(c) of draft article 7 of the Uniform Rules is based upon the detriment suffered by the addressee and the idea of restitution.

44. The focus of article 13 of the Model Law and draft article 7 of the Uniform Rules is different. Article 13 focuses upon attribution of the message while draft article 7 establishes a rule of liability for attribution of the signature. The Working Group may wish to recall the decision to be made under draft article 4 as to whether there is a legal need for a distinction to be drawn between attribution of the message and attribution of the signature (see above, para. 32). The relationship between the two draft articles may need to be considered to ensure that there is no confusion, in cases of a signed data message, as to which provision should be used to attribute the data message. One means of avoiding the potential for confusion would be to provide a specific rule applicable to cases in which the data message is signed with an [enhanced] electronic signature. Variant C of draft article 7 has been included for this purpose. In addition to the grounds of manifest unfairness, draft paragraph (3) of Variant C repeats the two instances provided by article 13 where the message cannot be attributed to the purported signer, while draft paragraph (4) of Variant C provides some guidance as to what may constitute manifest unfairness. The Working Group may like to consider other situations which might constitute manifest unfairness in the context of attribution.

Section III. Digital signatures supported by certificates

Article 8. Contents of [enhanced] certificates

Variant A

(1) For the purposes of these Rules, an [enhanced] certificate shall, as a minimum:

(a) identify the certification authority issuing it;

(b) name or identify the [signer][subject of the certificate] or a device or electronic agent under the control of [the signer] [the subject of the certificate] [that person];

(c) contain a public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(d) specify the operational period of the certificate;

(e) be digitally signed or otherwise secured by the certification authority issuing it;

[(f) specify restrictions, if any, on the scope of the use of the public key;]

[(g) identify the algorithm to be applied].

Variant B

(1) In disclosing to any party the information in a certificate, a certification authority [or the subject of a certificate] shall ensure that such information shall include, at least, that which is

set out in paragraph (2), except to the extent expressly otherwise agreed between the certification authority [or the subject, as the case may be] and such party.

Variant X

(2) The information referred to in paragraph (1) shall include:

(a) for all certificates,

(i) the identity of the certification authority using it;

(ii) the public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(iii) the digital or other signature of the certification authority issuing the certificate [the information];

(b) for [.....] certificates,

(i) the operational period of the certificate;

[(ii) the restrictions, if any, applicable to the scope of the use of the public key;]

[(iii) the identity of the algorithm to be applied].

Variant Y

(2) The information referred to in paragraph (1) shall include:

(a) the identity of the certification authority using [the certificate][the information];

(b) the name or identity of the [signer][subject of the certificate] or a device or electronic agent under the control of [the signer] [the subject of the certificate] [that person];

(c) the public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(d) the digital or other signature of the certification authority issuing the certificate [the information];

(3) Certificates may also include other information, including:

(a) the operational period of the certificate;

[(b) the restrictions, if any, applicable to the scope of the use of the public key;]

[(c) the identity of the algorithm to be applied].

References

A/CN.9/454, paras. 89-116;
A/CN.9/WG.IV/WP.76, para. 31;
A/CN.9/446, paras. 113-131 (draft article 8);
A/CN.9/WG.IV/WP.73, paras. 50-57;
A/CN.9/437, paras. 98-113 (draft article C); and
A/CN.9/WG.IV/WP.71, paras. 18-45 and 59-60.

Remarks

45. In view of the speed at which technology is changing and the development of forms of certification not based upon the three-party model (signer, relying party and certification authority), concern was expressed at the thirty-third session of the Working Group as to the appropriateness of including in these Rules a single provision dealing with the content of certificates (A/CN.9/454, paras. 90-97). This revision of draft article 8 includes the two variants which the Working Group agreed (A/CN.9/454, para 116) would provide the basis for future discussion.

46. Variant B reflects a concern that the issuing of a certificate might cover only the handing out of a certificate to the subject of the certificate, involving a contractual relationship, as opposed to disclosure of the information in the certificate to any relying third party. Variant B establishes an obligation to disclose certain information on a certificate, but this is not linked to any obligation to include that information in a certificate as a prerequisite to disclosure. Where any information is not included in a certificate, problems could arise if there is nevertheless an obligation to disclose such information. The Working Group may wish to consider whether it would be preferable to establish a provision which sets out the minimum information to be included in the certificate and a separate provision dealing with the obligation of disclosure.

Article 9. Effect of digital signatures supported by certificates

(1) In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature is an [enhanced] electronic signature if:

Variant A

(a) the digital signature was created during the operational period of a valid certificate and is [properly] verified [during the operational period of a valid certificate] by reference to the public key listed in the certificate;

(b) the certificate purports to bind a public key to [the signer's][a person's] [the originator's] identity;

(c) the certificate was issued for the purpose of supporting digital signatures which are [enhanced] electronic signatures; and

(d) the certificate was issued:

(i) by a certification authority licensed by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

(ii) by a certification authority accredited by a responsible accreditation authority applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics. A non-exclusive list of bodies or standards that comply with this paragraph may be published by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*; or

[(iii) in accordance with commercially appropriate and internationally recognized standards.]

Variant B

(a) the digital signature was [securely] created during the operational period of a valid certificate and is [properly] verified [during the operational period of a valid certificate] by reference to the public key listed in the certificate; and

(b) the certificate binds a public key to [the person's] [the originator's] [..] identity according to procedures established by:

(i) [*the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities*]; or

(ii) a responsible accreditation authority applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics; or

(iii) [international standards and commercial practices or usages widely known and regularly observed in the trade involved in the transaction].

(2) A digital signature that does not meet the requirements in paragraph (1) is regarded as an [enhanced] electronic signature if:

(a) sufficient evidence exists to indicate that:

(i) the certificate accurately binds the public key to the identity of the [subject of the certificate] [..]; and

(ii) the digital signature was properly created and verified [during the operational period of a valid certificate] using a trustworthy security procedure; or

(b) it qualifies as an [enhanced] electronic signature under other provisions of these Rules.

References

A/CN.9/454, paras. 117-138;
A/CN.9/WG.IV/WP.76, paras. 32-38;
A/CN.9/446, paras. 71-84 (draft article 5);
A/CN.9/WG.IV/WP.73, paras. 39-44; and
A/CN.9/437, paras. 43, 48 and 92

Remarks

47. Draft article 9 has been revised to reflect the decision of the Working Group at its thirty-third session (A/CN.9/454, para 136) that Variants A and B should be included in the text for future discussion. It sets out conditions that have to be met in order for a digital signature to be considered an [enhanced] electronic signature. [Enhanced] electronic signature is generally defined in draft article 1(b) as a signature which meets certain conditions. The Working Group may wish to consider whether the conditions in draft article 9 are additional to the general conditions of the definition, or intended to clarify and elaborate those conditions. The current version of draft article 9(2)(b), however, provides that a digital signature can be considered to be an [enhanced] electronic signature even if it does not meet the requirements of draft article 9(1), provided it qualifies as an [enhanced] electronic signature under other provisions of the Rules. This would include qualifying under the definition in draft article 1. If draft article 9 is not clearly drafted as an elaboration of the conditions set out in draft article 1, the Rules will establish two different standards for what is to be considered an [enhanced] electronic signature.

48. The Working Group may wish to consider draft article 9 in the context of draft article 1, with a particular focus on digital signature technology. The draft article could deal specifically, for example, with how a digital signature could satisfy the requirements of draft article 1(b) (i) to (iii).

CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES

Article 10. Undertaking upon issuance of [enhanced] certificate

(1) By issuing an [enhanced] certificate, the certification authority undertakes [to any person who reasonably relies on the [enhanced] certificate] that:

(a) the certification authority has complied with all applicable requirements of [these Rules];

(b) all information in the [enhanced] certificate is accurate as of the date it was issued, [unless the certification authority has stated in the [enhanced] certificate that the accuracy of specified information is not confirmed];

(c) to the certification authority's knowledge, there are no known, material facts omitted from the [enhanced] certificate which would adversely affect the reliability of the information in the [enhanced] certificate; and

[(d) that if the certification authority has published a certification practice statement, the [enhanced] certificate has been issued by the certification authority in accordance with that certification practice statement.]

(2) By issuing an [enhanced] certificate, the certification authority makes the following additional undertakings in respect of the [signer][subject] identified in the [enhanced] certificate [to any person who reasonably relies on the [enhanced] certificate]:

(a) that the public key and private key of the [signer][subject] identified in the [enhanced] certificate constitute a functioning key pair; and

(b) that at the time of issuing the [enhanced] certificate, the private key:

(i) corresponds to the [signer][subject] identified in the [enhanced] certificate; and

(ii) corresponds to the public key listed in the [enhanced] certificate.

References

A/CN.9/454, paras. 139-144;
A/CN.9/WG.IV/WP.76, para. 39;
A/CN.9/446, paras. 134-145 (draft article 10);
A/CN.9/WG.IV/WP.73, paras. 61-63;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

49. Draft article 10 reflects the decision made by the Working Group at its thirty-third session (A/CN.9/454, paras. 140-144), although the Working Group agreed that this article would need to be considered in the future in conjunction with draft articles 11 and 12.

50. The revised draft of article 10 is limited in its application to [enhanced] electronic signatures on the basis that prescribing a mandatory standard for all types of certificates may not be appropriate in view of the numerous types and uses of certificates that may develop.

Article 11. Contractual liability

(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other relying party having a contractual relationship with the certification authority], the rights and obligations of the parties [and any limitation thereon] are determined by their agreement [subject to applicable law].

(2) [Subject to article 10], a certification authority may, by agreement, exempt itself from liability for any loss resulting from reliance on the certificate. However, the clause which limits or excludes the liability of the certification authority may not be invoked to the extent that exclusion or limitation of contractual liability would [be grossly unfair] [be inherently unfair and lead to an evident imbalance between the parties][unjustifiably give one party an excessive advantage], having regard to the purpose of the contract and other relevant circumstances.

References

A/CN.9/454, paras. 145-157;
A/CN.9/WG.IV/WP.76, para. 40;
A/CN.9/446, paras. 146-154 (draft article 11);
A/CN.9/WG.IV/WP.73, paras. 64-65;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

51. Draft article 11 reflects the decision of the Working Group at its thirty-third session (A/CN.9/454, para. 149) to maintain an article along the lines of draft article 11 in the Uniform Rules. Concern was expressed at the session that the term "grossly unfair" would not be understood in all legal systems (A/CN.9/454, para. 152). The Working Group was reminded that paragraph (2) was inspired by the UNIDROIT Principles on International Commercial Contracts (Article 7.1.6) as an attempt to provide a uniform standard for assessing the general acceptability of exemption clauses. The reference to the limitation or exemption of liability being "grossly unfair" suggested a flexible approach to exemption clauses, with the aim of promoting a broader recognition of limitation and exemption clauses than would otherwise be the case if the Uniform Rules were to refer merely to the law applicable outside the Uniform Rules (A/CN.9/WG.IV/WP.73, para. 64). Additional words in square brackets have been included in order to better explain the term "grossly unfair". These words are taken from the explanatory material to article 7.1.6 of the UNIDROIT Principles.

Article 12. Liability of the certification authority to parties relying on certificates

(1) Subject to paragraph (2), where a certification authority issues a certificate, it is liable to any person who reasonably relies on that certificate for:

(a) errors in or omissions from the certificate, unless the certification authority proves that it or its agents have taken all reasonable measures to avoid errors in or omissions from the certificate;

(b) failure to register revocation of the certificate, unless the certification authority proves that it or its agents have taken all reasonable measures to register the revocation promptly upon receipt of notice of the revocation; and

(c) the consequences of not following any procedure set forth in the certification practice statement published by the certification authority.

(2) Reliance on a certificate is not reasonable to the extent that it is contrary to the information contained [or incorporated by reference] in the certificate [or in a revocation list] [or in the revocation information]. [Reliance is not reasonable, in particular, if [to the extent to which] it is:

(a) for a purpose contrary to the purpose for which the certificate was issued;

(b) in respect of a transaction, the value of which exceeds the value for which the certificate is valid; or

(c) [...].]"

References

A/CN.9/454, paras. 158-163;
A/CN.9/WG.IV/WP.76, para. 41;
A/CN.9/446, paras. 155-173 (draft article 12);
A/CN.9/WG.IV/WP.73, paras. 66-67;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

52. At its thirty-third session the Working Group agreed that draft articles 10, 11 and 12 would need to be considered together at a future meeting to ensure that obligations imposed upon certification authorities corresponded with the liability rules established by the Uniform Rules (A/CN.9/454, para. 159), but that draft article 12 should be retained and revised to reflect a number of drafting changes. These drafting changes have been made in this revision of draft article 12.

General remarks regarding draft articles 13-15

53. For lack of sufficient time, the Working Group had only a preliminary discussion of draft articles 13, 14 and 15 (A/CN.9/454, paras. 164-169). Some concerns were expressed about the level of detail of these draft articles and the technical assumptions upon which they were based. It was proposed at the Working Group that these draft articles should only be applicable to digital signatures and that, since they dealt with primary obligations of a certification authority, the substance of those obligations should be resolved before issues of liability could be considered. It was agreed that the draft articles should be retained in square brackets for future consideration.

[Article 13. Revocation of certificate

"(1) During the operational period of a certificate, the certification authority that issued the certificate must revoke the certificate in accordance with the policies and procedures governing revocation specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving:

(a) a request for revocation by the [signer] [subject] identified in the certificate, and confirmation that the person requesting revocation is the [rightful] [signer] [subject], or is an agent of the [signer] [subject] with authority to request the revocation;

(b) reliable evidence of the [signer's] [subject's] death if the [signer] [subject] is a natural person; or

(c) reliable evidence that the [signer] [subject] has been dissolved or has ceased to exist, if the [signer] [subject] is a corporate entity.

"(2) The [signer] [subject] in relation to a certified key pair is under an obligation to revoke, or to request revocation of, the corresponding certificate where the [signer] [subject] knows that the private key has been lost, compromised or is in danger of being misused in other respects. If the [signer] [subject] fails to revoke, or to request revocation of, the certificate in such a situation, the [signer] [subject] is liable to any person relying on a message as a result of the failure by the [signer] [subject] to undertake such revocation.

"(3) Regardless of whether the [signer] [subject] identified in the certificate consents to the revocation, the certification authority that issued a certificate must revoke the certificate promptly upon acquiring knowledge that:

(a) a material fact represented in the certificate is false;

(b) the certification authority's private key or information system was compromised in a manner affecting the reliability of the certificate; or

(c) the [signer's] [subject's] private key or information system was compromised.

"(4) Upon effecting the revocation of a certificate under paragraph (3), the certification authority must notify the [signer] [subject] and relying parties in accordance with the policies and procedures governing notice of revocation specified in the applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the [signer] [subject] and promptly publish notice of the revocation if the certificate was published, and otherwise disclose the fact of revocation upon inquiry by a relying party.

"(5) [As between the [signer] [subject] and the certification authority,] the revocation is effective from the time when it is [received] [registered] by the certification authority.

"[(6) As between the certification authority and any other relying party, the revocation is effective from the time it is [registered] [published] by the certification authority.]"]

[Article 14. Suspension of certificate

"During the operational period of a certificate, the certification authority that issued the certificate must suspend the certificate in accordance with the policies and procedures governing suspension specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving a request to that effect by a person whom the certification authority reasonably believes to be the [signer] [subject] identified in the certificate or a person authorized to act on behalf of that [signer] [subject]."]

[Article 15. Register of certificates

(1) Certification authorities shall keep a publicly accessible electronic register of certificates issued, indicating the time when any individual certificate expires or when it was suspended or revoked.

(2) The register shall be maintained by the certification authority.

Variant A for at least [30] [10] [5] years

Variant B for ... *[the enacting State specifies the period during which the relevant information should be maintained in the register]* after the date of revocation or expiry of the operational period of any certificate issued by that certification authority.

Variant C in accordance with the policies and procedures specified by the certification authority in the applicable certification practice statement.]

Notes

1. Official Records of the General Assembly, Fifty-first Session, Supplement No. 1 (A/51/17), paras. 223-224.

2. Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.